УДК 681.3

ДЕЯКІ АСПЕКТИ КРИПТОГРАФІЧНОГО АНАЛІЗУ БЛОКОВИХ МАТРИЧНИХ ПЕРЕТВОРЕНЬ

Вячеслав Василенко
Відкрите акціонерне товариство "КП ОТІ"

Анотація: **Розглядаються умови здійснення криптографічного аналізу блокових матричних перетворень із позиційної системи числення в систему лишкових класів та із системи умовних лишків у позиційну систему числення, а також умови забезпечення високої криптографічної стійкості таких перетворень.**
Summary: **The terms of realization of cryptographic analysis of sectional matrix transformations from the position scale of notation in the system of systems of remaining classes and from the system of conditional tailings in the position scale of notation, and also condition of providing of high cryptographic firmness of such transformations are examined.**
Ключові слова: **Інформація, інформаційний блок, конфіденційність, криптографічний аналіз, криптографічні перетворення, лишкові класи, матриця, системи числення.**

Вступ

Однією із вкрай важливих для сучасних автоматизованих систем є проблема забезпечення конфіденційності інформації [1 – 3], для вирішення якої застосовуються ті чи інші методи, методики чи алгоритми. Для забезпечення конфіденційності інформації в багатьох випадках криптографічне перетворення є чи не єдиним шляхом забезпечення її конфіденційності (з певною стійкістю до спроб розкриття її змісту – криптографічною стійкістю). На цей час теорія криптографічних перетворень розвинута досить широко й для забезпечення конфіденційності інформаційних об'єктів можна застосувати ті чи інші алгоритми криптографічного перетворення. Можливі варіанти таких алгоритмів, зокрема, блокових криптографічних перетворень на основі переводу із позиційної системи числення в систему лишкових класів, а також із системи лишкових класів у позиційну систему числення розглянуто в [4, 5]. При цьому переводу з однієї системи числення в іншу підлягають цифрові коди, якими в автоматизованих (комп'ютерних) системах представлені інформаційні об'єкти.

З урахуванням викладеного в [4] підходу, процедура (алгоритм) блокового криптографічного перетворення початкового n – символьного цифрового коду (блоку відкритого тексту) А із n символів в блок зашифрованого тексту – число $A_ш$ (на боці передавача інформації) і зворотного перетворення (на боці отримувача інформації) блоку зашифрованого тексту – числа $A_ш$ в блок відкритого тексту A зводиться до наступних операцій (функцій):

1. формування за правилами відповідного криптографічного перетворення кодувальної G та декодувальної матриць G^{-1} (в [5] розглянуті варіанти та можливості визначення однієї із цих матриць при відомій іншій);

2. представлення початкового тексту A у вигляді сукупності блоків A, B, C, ..., які підлягають криптографічному перетворенню; при цьому кожен із таких блоків, наприклад блок A, розглядається у вигляді матриці – рядка розмірності $(1 \times m)$ виду $A = (a_1, a_2, ..., a_i, ..., a_m)$;

3. здійснення на боці передавача інформації криптографічного перетворення кожного із блоків відкритого тексту, наприклад, блоку A: $A_ш = A \times G$ і отримання при цьому зашифрованого тексту $A_ш$, $B_ш$, $B_ш$, ..., який поблочно чи певним фрагментом (повідомленням, пакетом) передаються отримувачу;

4. здійснення на боці отримувача інформації зворотного перетворення $A = A_ш \times G^{-1}$, $B = B_ш \times G^{-1}$, $C = C_ш \times G^{-1}$, ...

Одним із шляхів створення загроз конфіденційності (загроз розкриття змісту інформаційних об'єктів) з боку порушників є використання недостатньо високої криптографічної стійкості застосованого перетворення і отримання ключів (механізмів) перетворення шляхом здійснення криптографічного аналізу фрагменту (фрагментів) відкритого тексту певної довжини та фрагменту (фрагментів) закритого (зашифрованого) тексту, який є відповідним відкритому.

У статті розглядаються деякі можливі аспекти криптографічного аналізу запропонованих в [4, 5] блокових матричних перетворень та шляхи підвищення, у разі необхідності, їх криптографічної стійкості.

І Оцінка можливостей криптографічного аналізу блокових криптографічних перетворень

Нехай для порушення конфіденційності криптоаналітик прагне отримати ключі, а в ще більш придатному варіанті – матриці прямого G чи/та зворотного G^{-1} криптографічних перетворень, за допомогою яких можна:

1. здійснювати дешифрування інформаційних об'єктів, адресованих даному утримувачу, а також інформаційних об'єктів, не призначених даному користувачеві (реалізуючи, наприклад, несанкціонований доступ неавторизованого користувача);

2. здійснювати шифрування інформаційних об'єктів, призначених для дезінформації користувачів, які користуються засобами шифрування з даними матрицями криптографічних перетворень, не знаючи, що система забезпечення конфіденційності є подоланою (несанкціонований доступ неавторизованого користувача).

Як відомо, для цього криптоаналізу піддаються певні фрагменти відкритого тексту та фрагменти закритого (зашифрованого) тексту, який є відповідним відкритому. Нехай такими фрагментами є блоки *A, B, C, ...* відкритого та $A_ш$, $B_ш$, $C_ш$, ... зашифрованого текстів. У результаті аналізу цих фрагментів криптоаналітику потрібно якимось чином отримати ключі (матриці прямого G чи/та зворотного G^{-1} криптографічних перетворень). Наразі можна сформувати, принаймні, дві таких можливості.

Перша можливість отримання ключів перетворення полягає у використанні певних особливостей застосованих кодових перетворень. Наприклад, при застосуванні перетворень із використанням системи лишкових класів можна використати можливість "статистичного" аналізу величин елементів (лишків по наборам основ) зашифрованого (при перетворенні типу позиційна система числення → система лишкових класів) та відкритого (при перетворенні типу система лишкових класів → позиційна система числення). Ця можливість ґрунтується на тому відомому факті, що максимальне значення величини лишку по будь-якій основі p_i дорівнює (p_i – 1). Тоді, маючи достатню вибірку (фрагмент закритого чи відкритого тексту – цифровий набір в системі лишкових класів), при умові знання місць розташування лишків по певним основам, визначити власне лишки (ключі перетворення) досить просто. Визначення місць розташування лишків по цим основам зводиться, в свою чергу, до знаходження таких інформаційних об'єктів, в яких є місця з концентрацією лишків лише по одній з основ. Такими інформаційними об'єктами є наразі сукупність блоків (фрагмент) тексту (не важливо відкритого чи закритого) у системі лишкових класів чи в системі умовних лишків, а також кодувальні (чи декодувальні) матриці при наявності можливостей з їх отримання. В обох випадках можливість визначення лишків (ключів перетворення) залежить від достатності обсягу цих вибірок для статистичного аналізу.

Друга можливість полягає в отриманні матриць прямого G чи/та зворотного G^{-1} криптографічних перетворень шляхом використання матричних операцій над фрагментами відкритого та зашифрованого текстів. Для цього будемо розглядати кожен із блоків *A, B, C, ...* рядком матриці $\overset{\nu}{A}$ (підматрицею з розмірністю $1\times m$) відкритого, а кожен із блоків $A_ш$, $B_ш$, $C_ш$, ... рядком (підматрицею з такою ж розмірністю) матриці $\overset{\nu}{A}_ш$ зашифрованого текстів. Наприклад, перший рядок матриці $\overset{\nu}{A}$ складе перший блок початкового тексту $A = (a_1, a_2, a_3, ..., a_m)$, другий рядок – блок початкового тексту B і т. д. При такому підході кожна із матриць $\overset{\nu}{A}$ і $\overset{\nu}{A}_ш$ складається із m рядків і m стовпців, тобто має розмірність $m\times m$:

$$\overset{\nu}{A} = \begin{pmatrix} a_1 & a_2 & a_3 & ... & a_m \\ b_1 & b_2 & b_3 & ... & b_m \\ c_1 & c_2 & c_3 & ... & c_m \\ ... & ... & ... & ... & ... \\ z_1 & z_2 & z_3 & ... & z_m \end{pmatrix}, \quad \overset{\nu}{A}_ш = \begin{pmatrix} a_{1ш} & a_{2ш} & a_{3ш} & ... & a_{mш} \\ b_{1ш} & b_{2ш} & b_{3ш} & ... & b_{mш} \\ c_{1ш} & c_{2ш} & c_{3ш} & ... & c_{mш} \\ ... & ... & ... & ... & ... \\ z_{1ш} & z_{2ш} & z_{3ш} & ... & z_{mш} \end{pmatrix}.$$

Тоді з урахуванням викладених в [4] підходів можна вважати, що криптографічні перетворення (шифрування) початкового тексту (матриці відкритого тексту) здійснені шляхом перемноження матриці $\overset{\nu}{A}$ і кодувальної матриці $\overset{\nu}{G}$:

$$\overset{\rho}{G} = \begin{pmatrix} g_{11} & g_{12} & g_{13} & \cdots & g_{1m} \\ g_{21} & g_{22} & g_{23} & \cdots & g_{2m} \\ g_{31} & g_{32} & g_{33} & \cdots & g_{3m} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ g_{n1} & g_{n2} & g_{n3} & \cdots & g_{mm} \end{pmatrix}.$$

Зворотне перетворення можна здійснити шляхом перемноження матриці $\overset{\nu}{A}_{ш}$ на декодувальну матрицю $\overset{\nu}{G}^{-1}$.

$$\overset{\rho}{G}^{-1} = \begin{pmatrix} g_{11}^{-1} & g_{12}^{-1} & g_{13}^{-1} & \cdots & g_{1m}^{-1} \\ g_{21}^{-1} & g_{22}^{-1} & g_{23}^{-1} & \cdots & g_{2m}^{-1} \\ g_{31}^{-1} & g_{32}^{-1} & g_{33}^{-1} & \cdots & g_{3m}^{-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ g_{n1}^{-1} & g_{n2}^{-1} & g_{n3}^{-1} & \cdots & g_{mm}^{-1} \end{pmatrix}.$$

Тобто

$$\overset{\nu}{A}_{ш} = \overset{\nu}{A} \times \overset{\nu}{G}, \ \overset{\nu}{A} = \overset{\nu}{A}_{ш} \times \overset{\nu}{G}^{-1}. \qquad (1)$$

Нагадаємо також, що правила вибору чи формування елементів кодувальної та декодувальної матриць визначаються типом перетворення. Якщо механізм формування елементів цих матриць є секретним, чи механізм формування елементів кодувальної матриці є загальновідомим, але при їхньому формуванні використовуються деякий секретний параметр – ключ, то зашифрований код має певну криптографічну стійкість, тобто стійкість до спроб одержати з зашифрованого коду (часто з використанням певної частки відкритого початкового тексту) ключ, кодувальну матрицю чи власне вихідний код (текст). Така криптографічна стійкість є основною властивістю таких перетворень і досить часто визначається числом варіантів ключів.

Аналіз виразів (1) дає змогу підмітити, що в разі наявності можливості обрахування зворотних матриць для фрагментів початкового та зашифрованого текстів $\overset{\nu}{A}^{-1}$ та $\overset{\nu}{A}_{ш}^{-1}$ нескладно отримати власне кодувальну чи декодувальну матриці. З цією метою досить помножити (зліва) кожен із виразів (1) на матриці для фрагментів початкового та зашифрованого текстів $\overset{\nu}{A}^{-1}$ та $\overset{\nu}{A}_{ш}^{-1}$:

$$\overset{\nu}{G} = \overset{\nu}{A}^{-1} \times \overset{\nu}{A}_{ш} = \overset{\nu}{A}^{-1} \times \overset{\nu}{A} \times \overset{\nu}{G} = E \times \overset{\nu}{G},$$

$$\overset{\nu}{G}^{-1} = \overset{\nu}{A}_{ш}^{-1} \times \overset{\nu}{A} = \overset{\nu}{A}_{ш}^{-1} \times \overset{\nu}{A}_{ш} \times \overset{\nu}{G}^{-1} = E \times \overset{\nu}{G}^{-1},$$

де E – одинична матриця.

Таким чином, з погляду загально теоретичних підходів задача розкриття механізму матричного блокового криптографічного перетворення, а відтак, і задача порушення конфіденційності інформаційних об'єктів може бути вирішеною.

II Можливості забезпечення стійкості суто криптографічних блокових перетворень

Запропоновані в [4, 5] механізми блокових матричних перетворень інформаційних об'єктів дають змогу здійснювати суто криптографічні перетворення, завадостійкі криптографічні перетворення (завадостійка криптографія) та завадостійке кодування (з використанням коду умовних лишків).

На початку розглянемо можливості забезпечення стійкості типів блокових суто криптографічних перетворень, викладених в [5]: позиційна система числення (ПСЧ) → система лишкових класів (СЛК) та система умовних лишків (СУЛ) → ПСЧ. Із попереднього розділу зрозуміло, що для забезпечення стійкості блокових криптографічних перетворень необхідно створити умови, коли, по-перше, виключена можливість визначення ключів перетворення з використанням "статистичного" аналізу величин елементів (лишків по наборам основ – елементам ключового набору) із фрагментів зашифрованого тексту, і, по-друге, коли обрахування (чи взагалі – існування) зворотних матриць $\overset{\nu}{A}^{-1}$ та $\overset{\nu}{A}_{ш}^{-1}$ з тих чи інших причин є неможливим.

Відмітимо, що можливостей "статистичного" аналізу при перетворенні типу СУЛ → ПСЧ не існує, іншими словами, таке перетворення є стійким щодо "статистичного" аналізу. Це пов'язано з тим, що елементи відкритого тексту розглядаються лише як умовні лишки (без будь-яких модифікацій цих

елементів), а величини власне основ системи числення залежать від цих елементів тільки через нерівність $p_i > (g - 1)$, де p_i – i-та основа СУЛ, а g – основа системи числення, в якій представлено елементи тексту (наприклад, $g = 256$ при байтовому представленні елементів початкового тексту). Тобто за значеннями відкритого тексту неможливо визначити елементи ключа перетворення. При перетвореннях же із ПСЧ в СЛК величини отриманих при цьому лишків знаходяться в інтервалі $[0, (p_i-1)]$, що за наявності достатньої статистики дає змогу визначати всі величини елементів ключа p_i ($i = 1, 2, ..., n$).

Для виключення можливості такого "статистичного" криптоаналізу елементів фрагменту зашифрованого тексту в СЛК при перетвореннях типу ПСЧ → СЛК є достатнім "викривлення" цих елементів шляхом, наприклад, порозрядного додавання за модулем 2 (існують і інші можливості "викривлень") до відповідного блоку такого блоку (матриці – рядка), який "викривлює" і є таємним для порушника (в даному випадку – криптоаналітика), але є відомим як відправнику, так і отримувачу повідомлення. Такий блок (матриця – рядок), який "викривлює", може складатися, наприклад, із ключових елементів. Перед виконанням усіх необхідних операцій з такими блоками (матрицями – рядками) достатньо здійснити ще одне порозрядне додавання за модулем 2 до цього блоку такого ж самого "викривлюючого" блоку (матриці – рядка) і зняти, тим самим, попереднє викривлення. Таким чином, стійкість і останнього перетворення щодо "статистичного" аналізу забезпечується досить просто.

Перед розглядом умов обрахування (чи взагалі – існування) зворотних матриць $\overset{\rho}{A}^{-1}$ та $\overset{\rho}{A}_{ш}^{-1}$ нагадаємо [5], що при використанні перетворень типу ПСЧ → СЛК та СЛК → ПСЧ для забезпечення однозначності перетворень необхідно узгодити діапазони представлення вихідних та перетворених чисел (під числом тут та надалі будемо розуміти цифровий еквівалент відповідного коду – початкового блоку А чи зашифрованого блоку $А_ш$), тобто необхідно забезпечити виконання умови $g^{m-1} \le P$, де g – основа системи числення, яка використана для подальших математичних операцій над цими цифровими кодами ($g = 2$ для двійкового,
$g = 10$ для десяткового представлення, $g = 256$ для байтового представлення та т. п.), m – кількість символів початкового блоку, $P = \prod_{j=1}^{n} p_j$ – діапазон представлення ("робочий" діапазон) СЛК. Окрім того, для забезпечення можливостей блокових матричних перетворень слід узгодити й розміри матриць (довжини блоку) – розмірності матриці вихідної інформації (m) і розмірності кодувальної матриці (n), а також розмірностей блоку зашифрованого тексту і розмірності декодувальної матриці. Остання вимога призводить до необхідності якимось чином забезпечити рівність $m = n$, що, зрозуміло, може здійснюватися, залежно від умов, шляхом збільшення чи то m, чи то n.

З урахуванням цих зауважень відзначимо, що умовами для неможливості обрахування чи існування певних матриць при перетвореннях типу ПСЧ → СЛК є:

1. Наявність в матрицях однакових (наприклад, нульових) рядків чи стовпців, коли виконується умова, при якій визначник матриці дорівнює нулю ($\det \overset{\rho}{A} = 0$), що має своїм наслідком відсутність зворотних матриць. В [5] наведено умови здійснення блокових криптографічних перетворень з використанням лишкових класів (перетворення типу ПСЧ → СЛК). Показано, що під час шифрування при $m < n$ згадане вище узгодження може здійснюватися, наприклад, шляхом доповнення блоків початкового тексту, який підлягає перетворенню (збільшення розміру матриці початкового блоку розмірності $1 \times m$), до розмірності $1 \times n$. Це забезпечується тим, що вихідні блоки (матриці – рядки) $A = (a_1, a_2, ..., a_i, ..., a_m)$ можуть доповнюватися потрібною кількістю нулів ($s = n - m$) на місцях старших розрядних коефіцієнтів. В цьому випадку матриці-рядки A набувають вигляду $A = (0, 0, ..., a_1, a_2, ..., a_i, ..., a_m)$. Зрозуміло, що при зворотному перетворенні (дешифруванні) результат дешифрування також буде мати таку ж кількість нулів (нульових стовпців чи рядків). Звідсіля витікає, що, по-перше, для створення умови, коли $m < n$, як основи системи числення в лишкових класах вибираються взаємно прості числа, починаючи із найменших. Тоді створюються умови для забезпечення $n > m$. По друге, в разі неможливості забезпечення умови $m < n$ за рахунок вибору малих значень основ СЛК, можна їх кількість збільшити штучно. При цих умовах отримати зворотні матриці $\overset{\rho}{A}^{-1}$ та $\overset{\rho}{A}_{ш}^{-1}$ із фрагментів відкритого та відповідного йому закритого текстів є неможливим.

2. Розміри фрагментів відкритого та відповідного йому зашифрованого тексту є недостатніми для побудови матриць $\overset{\rho}{A}$, $\overset{\rho}{A}_{ш}$. Зрозуміло, що така можливість існує, коли кількість блоків у згаданих фрагментах є меншою, ніж n. Слід зазначити, що при цьому розв'язання відповідних матричних рівнянь

має безліч рішень.

Примітка 1. Забезпечити останнє можливо при умові зміни матриць перетворення (чи сеансових ключів для їх формування) з періодичністю, яка відповідає шифруванню/дешифруванню не більше ніж (n – 1) блоків зашифрованого тексту.

Тобто при дотриманні умов, розглянутих вище, здійснення криптоаналізу перетворення ПСЧ → СЛК через отримання кодуючих чи декодуючих матриць шляхом перетворення фрагментів відкритого та зашифрованого текстів стає неможливим.

При перетвореннях типу СУЛ → ПСЧ для створення умов, коли обрахування (чи взагалі – існування) зворотних матриць $\overset{\cup}{A}^{-1}$ та $\overset{\cup}{A}_{ш}^{-1}$ з тих чи інших причин є неможливим, слід враховувати наступне. Для забезпечення можливості такого перетворення усі символи початкового блока для шифрування

$A = \alpha_1, \alpha_2, \ldots, \alpha_m$,

слід [5] уявляти символами в деякій умовній СЛК – лишками за основами p_i (i = 1, 2, ..., m). Щоб символи початкової системи числення можна було вважати символами в умовній СЛК значення основ цієї умовної СЛК p_i потрібно вибирати із умови

$$p_i > g^f,$$

де g – основа вихідної (позиційної) системи числення, а f – розрядність символів початкової системи числення.

Ця вимога пов'язана з тим, що в СЛК значення основ є завжди більшими ніж значення лишків (а це – значення символів початкової системи числення) за цими основами. За рахунок цього завжди виконується умова $g^{m-1} \le P = \prod_{j=1}^{m} p_j$. Таким чином, кількість лишків у такій умовній СЛК завжди дорівнює числу символів у блоці початкового коду. Звідсіля витікає, що для підвищення криптографічної стійкості перетворень типу ПСЧ → СЛК слід штучно вводити r додаткових основ (r = 1, 2, ...) і збільшувати до $n = m + r$ розмірності матриць – рядків блоків вхідного та перетвореного текстів, а також кодувальної та декодувальної матриць. При цьому, як і для перетворення ПСЧ → СЛК, **здійснення криптоаналізу через отримання кодуючих чи декодуючих матриць шляхом перетворення фрагментів відкритого та зашифрованого текстів стає неможливим**.

III Можливості забезпечення стійкості завадостійких криптографічних перетворень

При використанні завадостійкого криптографічного перетворення (завадостійкої криптографії) кодувальна матриця G_1 складається [4] із підматриці G розмірності ($n \times n$), за допомогою якої здійснюється криптографічне перетворення блоків початкового відкритого тексту, і $r = (k - n)$ додаткових стовпців і рядків, призначених для забезпечення контролю наявності будь-яких викривлень. Місце розташування цих додаткових стовпців і рядків для подальших міркувань не має значення. Нехай ця матриця має вигляд:

$$G_1 = \begin{pmatrix} g_{11} & g_{12} & \cdot & g_{1n} & \cdot & g_{1k} \\ g_{21} & g_{22} & \cdot & g_{2n} & \cdot & g_{2k} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ g_{n1} & g_{n2} & \cdot & g_{nn} & \cdot & g_{nk} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ g_{k1} & g_{k2} & \cdot & \cdot & \cdot & g_{kk} \end{pmatrix} \leftarrow \text{Підматриця } G \ (n \times n) \ .$$

При виконанні вже розглянутих у другому розділі умов щодо захисту від "статистичного" аналізу, а також щодо побудови кодувальних та декодувальних матриць (G та $\overset{\cup}{G}^{-1}$), така побудова кодувальної (і, відповідно, декодувальної) матриці пояснюється тим, що описані вище варіанти перетворення забезпечують надзвичайно важливу властивість захищеності інформації – конфіденційність, однак не дозволяють вирішувати задачу контролю, а тим більше, відновлення цілісності інформації. Це пов'язано з тим, що операція обчислення зашифрованого блоку $A_ш = A \times G$ не приводить до збільшення в закодованому слові кількості інформації (появи в ньому нової інформації), необхідної для наступного

виявлення факту викривлення, місця викривлення і його величини.

Отже, для перетворень, що дозволяють здійснювати не лише криптографічні перетворення, а й контроль цілісності (можливо з наступним її відновленням) необхідно в блоки початкового тексту додатково ввести потрібну для цього надлишковість, тобто використовувати матриці-рядки – блоки початкового тексту довжиною k символів ($k = n + r$), а також кодувальну матрицю розмірності ($k \times k$). Додаткові r стовпців кодувальної матриці мають забезпечити формування в блоці перетвореної інформації надлишковості за правилами певного завадостійкого, наприклад, циклічного чи іншого (див. нижче) коду. Тоді, внаслідок множення матриці-рядку A на кодувальну матрицю G_1 n символів початкового блоку перетворяться в закодований блок з властивостями завадостійкого коду, довжиною k символів, що дозволяє при зворотних перетвореннях виявити факт наявності, а при певному виборі надлишковості, – і місця викривлення. Із викладеного раніше зрозуміло, що, з метою **убезпечення як кодувальної, так і декодувальної матриць від можливості розкриття,** r додаткових символів матриці-рядка (початкового блоку) мають бути однаковими, наприклад, нульовими.

IV Можливості забезпечення криптографічної стійкості завадостійкого кодування (контролю цілісності)

Описані в другому розділі перетворення забезпечують надзвичайно важливу властивість захищеності інформації – конфіденційність, а описані в третьому розділі – як конфіденційність, так і цілісність одночасно.

Однак, досить розповсюдженим є варіант, коли необхідно здійснювати лише контроль цілісності (можливо з наступним її відновленням) інформації без її криптографічного перетворення.

Даний варіант передбачає розширення початкового коду довжиною в n символів до початкового слова для кодування довжиною в k символів і використання кодувальної матриці спеціального виду – матриці, що породжує (у термінах завадостійкого кодування). Матриця, що породжує, у цьому випадку як підматриця G містить одиничну матрицю E і r додаткових рядків і стовпців ($r = k - n$), елементи яких визначаються необхідними властивостями (типом) завадостійкого коду:

$$G_2 = \begin{pmatrix} 1 & 0 & . & 0 & . & g_{1k} \\ 0 & 1 & . & 0 & . & g_{2k} \\ . & . & . & . & . & . \\ 0 & 0 & . & 1 & . & g_{nk} \\ . & . & . & . & . & . \\ 0 & 0 & . & . & . & 1 \end{pmatrix}$$

Одинична підматриця E . $(n \times n)$

У результаті множення початкового слова для кодування на кодувальну матрицю G_2 одержують k – символьний код, у якому перші n елементів збігаються з відповідними елементами початкового коду, а інформація, що формується в додаткових, надлишкових r символах закодованого слова в теорії завадостійкого кодування, зветься контрольною ознакою і використовується для контролю наявності викривлень.

Якщо, наприклад, використовувати кодувальну матрицю, у якій r = 1, а n елементів k – го стовпця дорівнюють одиниці (тобто $g_{ik} = 1$ для усіх i), то одержимо завадостійкий код, у якому контрольну ознаку отримують шляхом підсумовування (наприклад, порозрядного логічного чи за модулем 2^b, де b – двійкова довжина символів початкового коду, тобто його довжина в бітах, і т. д.) усіх n елементів початкового коду (еквівалент контрольного підсумовування). При зворотному перетворенні (контролі наявності викривлень) здійснюють множення закодованого слова на перевірочну матрицю G_2^{-1}, внаслідок чого одержують вектор-рядок із n інформаційних символів (можливо з викривленнями) та r, так званих, синдромів викривлень, елементи яких при виборі надмірності, достатній для рішення задач корекції, несуть інформацію про наявність, місце і величину викривлень в інформаційному блоці, що перевіряється. При недостатній надмірності ці елементи несуть інформацію про місце чи просто про наявність викривлень (коди, що виявляють). Звернемо увагу на те, що при такому виборі елементів стовпців, мова може йти лише про ту властивість подібних завадостійких кодів, яка забезпечує виявлення (і, можливо, усунення) тих викривлень в інформаційних блоках, які не мають навмисного характеру. Це пов'язано з абсолютно відкритими (відомими для усіх бажаючих) елементами матриці G_2, а отже і абсолютно відкритими процедурами формування контрольних ознак. Тобто не можна вести мову про криптографічну стійкість таких перетворень та їх застосовування для контролю цілісності.

Зрозуміло, що при використанні кодів даного типу для контролю цілісності слід використовувати секретні (невідомі для усіх бажаючих) елементи матриці G_2. Приклад застосування такого коду (ЛУ – коду, коду умовних лишків) досить детально надано в [4]. В цьому випадку елементи початкового блоку для кодування розглядаються як умовні лишки від ділення деякого числа на основи СУЛ p_i (вимоги до цих величин викладено вище), а елементами останнього (*k*-го) стовпчика цієї матриці (будемо виходити із умов наведених в [4] прикладів, тобто для $r = 1$) є величини $g_{ik} = m_i / p_i$, де m_i – константи цієї системи числення ("ваги" ортогональних базисів). Внаслідок множення початкового блоку A на матрицю G_2 буде отримано блок $A_ш$, перші n елементів якого збігаються із відповідними елементами блоку A, а порядок обчислення останнього елементу детально викладено в [4] (після нескладних перетворень результату множення блоку A на останній стовпчик матриці G_2 ($\sum_{i=1}^{n} \alpha_i \cdot m_i / p_i$) отримується лишок в СУЛ α_k від ділення на контрольну основу p_k деякого умовного числа $\overline{A}$).

В разі, коли константи СУЛ, зокрема величина контрольної основи, вибрані правильно і елементи останнього стовпчика матриці G_2 зберігаються в секреті, потенційний порушник не має змоги обчислити для блоку A таке ж саме значення α_k, що дає змогу вирішувати задачі як контролю, так і поновлення цілісності інформаційних об'єктів. Неважко помітити, що для цього механізму можливості розкриття констант СУЛ шляхом "статистичного" аналізу відсутні. Лишаються спроби їх розкриття шляхом обчислення відповідних зворотних матриць з використанням фрагментів відкритого та "зашифрованого" (мається на увазі лише величина α_k) тексту. Як боротися з такими спробами, розглянуто вище.

V Аналіз можливостей криптоаналізу блокових матричних перетворень шляхом прямого перебору ключів

Розглянуті в попередніх розділах результати аналізу можливостей забезпечення криптографічної стійкості механізмів блокових матричних перетворень дають можливість стверджувати, що способи криптоаналізу як шляхом "статистичного" аналізу з використанням фрагментів відкритого та зашифрованого тексту, так і шляхом обрахування прямих чи зворотних матриць при дотриманні викладених у відповідних розділах рекомендацій, є не результативними. Таким чином, на погляд автора, єдиним шляхом розкриття елементів ключа (чи, що є тим же самим, елементів матриць для перетворення) залишається спосіб прямого перебору, а криптографічна стійкість визначається тоді кількістю варіантів ключових наборів.

Як приклад, розглянемо варіант визначення кількості варіантів ключових наборів для умов контролю цілісності вихідних інформаційних блоків, довжиною до $n = 32$ символів кожен, у разі використання перетворень, коли при формуванні контрольних ознак вихідні блоки тексту вважаються числами в системі умовних лишків. При цьому врахуємо, що перетворення для всіх розглянутих методів здійснюються з використанням n "робочих" та r "контрольних" основ, які вибираються з множини взаємно простих чисел.

Нехай символами початкового тексту є байти, а як контрольні основи (з умови технологічності програмної реалізації) необхідно використовувати складену контрольну основу з s взаємно простих чисел з проміжку [131, ..., 251], оскільки їх розрядність також повинна бути рівною 8 бітам (по 1 байту кожна). Неважко переконатися, що кількість таких чисел дорівнює 29. Робочі основи, виходячи з умови забезпечення восьмибітових умовних лишків, якими є символи початкового тексту, слід вибирати розрядністю більшою, ніж 8. Тобто такими основами можуть бути взаємно прості числа, величина яких перевищує 257.

Якщо вибирати ці основи із діапазону взаємно простих чисел [257, 1579], то їх кількість налічує 195. Якщо при контролі та поновленні цілісності використовується n із 195 робочих та s із 29 контрольних основ, то загальна кількість $N_{вк}$ варіантів ключів визначається як добуток кількості перестановок (розміщень) із 195 елементів по n на кількість перестановок (розміщень) із 29 елементів по s:

$$N_{вк} = A_{195}^{n} \cdot A_{29}^{s}.$$

При застосуванні цього механізму лише для контролю цілісності обмеженням на величини робочих основ є лише можливості процесорів з обробки багатобайтових чисел, тому кількість простих чисел (потенційних основ) є значно більшою. Наприклад, кількість простих чисел, що є більшими за 256 і меншими за 6000 перевищує 650. Тому і кількість варіантів є значною. Нижче в таблиці для порівняння

наведено кількість варіантів ключів для відомих механізмів формування цифрового підпису (за стандартом ГОСТ 34.310 – 94), та функції хешування (за стандартом ГОСТ 34.311-95), а також запропонованого механізму.

Таблиця – Кількість варіантів ключових наборів для різних механізмів формування контрольних ознак

Довжина ключа (байти)	Механізми формування хеш–функцій (контрольних ознак) для контролю цілісності інформації		
	ГОСТ 34.310 – 94	ГОСТ 28147-89	ЛУ – код, n = 32, s = 4
32	-	10^{76}	»10^{76}
64	$9{,}45\cdot10^{65}$	-	>10^{136}
128	$9{,}45\cdot10^{156}$	-	» 10^{260}

Примітка 2. Для другої та третьої колонок використані дані Інституту Інформаційних Технологій Харківського технічного університету радіоелектроніки (в другій колонці, виходячи з обсягу обчислень в $3\cdot10^5$ та $3\cdot10^{12}$ міпсороків відповідно). В четвертій колонці наведено дані для довжини інформаційної частки базового кодового слова в 32 байти та довжини надлишкової частки базового кодового слова в 4 байти.

До речі при застосуванні цього механізму лише для контролю цілісності можна суттєво зменшити об’єм надлишкової інформації та спростити саму процедуру формування контрольних ознак. Це пов’язане з тим, що сформована за розглянутою процедурою надлишкова сукупність контрольних ознак містить в собі інформацію, потрібну для визначення в подальшому наявності викривлення, його місця та величини. При контролі ж лише цілісності достатньо мати інформацію, потрібну для визначення в подальшому тільки наявності викривлення. При цьому під час формування контрольних ознак для інформаційних об’єктів значного обсягу (більше ніж 32 байти) можна поруч з конкатенацією використовувати і операції порозрядного додавання за модулем 2. За рахунок цього довжина контрольних ознак (об’єм надлишкової інформації) легко доводиться до довжини, визначеної міждержавним стандартом ГОСТ 34.311-95 [6].

Як видно з таблиці, запропонований механізм забезпечує кількість варіантів ключів, яка суттєво перевищує кількість варіантів ключів відомих механізмів, та має, відповідно, значно вищу імітостійкість. У наведених прикладах кількість варіантів ключів задовольняє вимогам навіть гарантованого криптозахисту.

Висновок

Аналіз криптографічної стійкості механізмів блокових матричних перетворень дає можливість стверджувати, що способи криптоаналізу шляхом “статистичного” аналізу з використанням фрагментів відкритого та зашифрованого тексту, спроби обрахування прямих чи зворотних матриць, при дотриманні викладених у відповідних розділах рекомендацій, є не результативними, а кількість варіантів ключових наборів є не меншою, ніж для інших відомих механізмів формування контрольних ознак.

*Література: **1.** Нормативний документ Системи технічного захисту інформації “Загальні положення про захист інформації в комп'ютерних системах від несанкціонованого доступу” (НД ТЗІ 1.1 – 002 – 99). **2.** Нормативний документ Системи технічного захисту інформації “Критерії оцінки захищеності інформації в комп'ютерних системах від НСД” (НД ТЗІ 2.5 – 004 – 99). **3.** Нормативний документ Системи технічного захисту інформації “Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу” (НД ТЗІ 2.5.–005 –99). **4.** Василенко В. С. Варіант завадостійкого криптографічного перетворення // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні, вип. 8, 2004 р. –с. 101 – 108. **5.** Василенко В. С. Блокові криптографічні перетворення з використанням лишкових класів // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні, вип. 10, 2005 р. – с. 99 – 105. **6.** Будько М. М., Василенко В. С., Короленко М. П. Проблеми забезпечення цілісності інформації в телекомунікаціях. // Правове, нормативне та метрологічне забезпечення Системи захисту інформації в Україні, 2000 р. – с. 123-129.*